Committee on
HOMELAND SECURITY
Chairman Michael McCaul

Opening Statement

July 18, 2013

Media Contact: Charlotte Sellmyer
(202) 226-8417

Statement of Subcommittee Chairman Patrick Meehan (R-PA)
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security

"Oversight of Executive Order 13636 and Development of the Cybersecurity Framework"

July 18, 2013
Remarks as Prepared

I would like to welcome everyone to today's hearing, which continues our Subcommittee's efforts to provide oversight over the President's cybersecurity Executive Order 13636. The focus of the Executive Order is to provide protection for our nation's critical infrastructure sectors from cyber threats. These sectors include our energy and nuclear facilities, our nation's transportation systems, our defense industrial base, and financial services among others.

Today we will focus on the Cybersecurity Framework, under which the National Institute of Standards and Technology (NIST) has the responsibility of working with stakeholders to develop.

The Framework is expected to be completed and released in October 2013. On July 1st, NIST released an outline of the framework, which will be the basis of the committee's questioning today.

So far NIST has held three workshops to gather input from industry, academia, and other stakeholders, with a fourth expected in September.

I believe that the outline of NIST's framework provides an important step to increasing our nation's awareness and ability to protect our networks from crippling cyber attacks. In fact, I

believe that there are many mature actors in both government and the private sector working in great coordination currently – including those at the Department of Homeland Security – to shield our systems from cyber threats. It is, however, those outliers – the ones without the awareness, those with insufficient resources – who can present immense vulnerabilities to entire networks. It is this concern that our subcommittee seeks to have allayed. We must find answers to the question of, how do we incentivize participation without creating counterproductive, onerous standards and regulations?

Adopting the NIST framework should result in a positive exercise for owners and operators of critical infrastructure. However, I have concerns that a self-assessment may not be sufficient to incentivize action to bolster cyber defenses.

Our committee has held over 200 meetings with stakeholders and one of the common themes emanating from our discussions is that they are only as strong as their weakest links. I believe an analysis of the incentives included in this framework is in order, and I look forward to hearing from the panel today on ways we can assist both the public and private sector to increase their hygiene with limited resources.

Providing incentives for organizations to share information and best practices is further complicated by the absence of liability protections in the Executive Order. Our goal should be to encourage threat information sharing, and I have questions about the ability of regulators to require use of the framework, turning this into burdensome "check-the-box" rules and regulations.

Ultimately, I believe it is the consensus of this committee that Congress must pass legislation, in order to address many of these outstanding issues. Existing structures within DHS must be authorized by Congress to continue functioning. Liability protections, information-sharing provisions, and industry-led incentives can only be fully enacted by statute, not presidential directives.

I look forward to working with the committee, with our panel, and DHS to craft legislation that will address these issues. I thank the panel for their participation today and I look forward to hearing your testimonies.

###